SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: 0072104455

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
SP4703-18-C-0507	2018 APR 09			

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME

9. ISSUED BY — CODE: SP4703

DCSO RICHMOND
8000 JEFFERSON DAVIS HWY
RICHMOND VA 23297-5441
USA
Local Admin: Allison Douglewicz PZGCD41 Tel: 804-279-2915 Fax: 804-279-2562
Email: Allison.Douglewicz@dla.mil

10. THIS ACQUISITION IS

- ☐ UNRESTRICTED OR ☒ SET ASIDE: _____ % FOR:
- ☐ SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ HUBZONE SMALL BUSINESS
- ☐ EDWOSB — NAICS: 541611
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☒ 8 (A) — SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☐ SEE SCHEDULE	Net 30 days	☒	DO-C9 / ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO — CODE:

SEE SCHEDULE

16. ADMINISTERED BY — CODE: SP4703

SEE BLOCK 9
Criticality: C PAS: None

17a. CONTRACTOR/ OFFEROR — CODE: 5C6G0 — FACILITY CODE:

VIZZ LIMITED LIABILITY COMPANY
3 W Garden Street Suite 407
PENSACOLA FL 32502-5633
USA

TELEPHONE NO. 8503616842

18a. PAYMENT WILL BE MADE BY — CODE: SL4701

DEF FIN AND ACCOUNTING SVC
BSM
P O BOX 182317
COLUMBUS OH 43218-2317
USA

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	See Schedule				

25. ACCOUNTING AND APPROPRIATION DATA

AA: 97X4930 5CBX 1000024 001 2520 S33189 $1555510.40

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

$1,555,510.40

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED 0000-00-00. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH , HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	Allison R. Douglewicz

30b. NAME AND TITLE OF SIGNER *(Type or Print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or Print)*	31c. DATE SIGNED
		Allison Douglewicz Allison.Douglewicz@dla.mil PZGCD41	2018 MAR 27

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

DLA Aviation BA Strategic Support Initiatives

SBA Requirement Number: 0491-18-801188

VIZZ, LLC's proposal submitted on February 27,2018 is hereby incorporated by reference. This is a Firm Fixed Price Contract. All terms and conditions of RFP SP4703-18-R-0011 apply an are incorporated by reference.

Schedule B:

BASE PERIOD (4/9/2018 - 4/8/2019)
CLIN 0001 Labor $1,551,110.40
CLIN 0002 Travel $ 4,400.00
Base Total: $1,555,510.40

OPTION PERIOD 1 (4/9/2019 - 4/8/2020)
CLIN 0003 Labor $1,589,376.00
CLIN 0004 Travel $ 10,000.00
Option Period 1 Total: $1,599,376.00

TOTAL PRICE (Base & Option) $3,154,886.40

NOTE: To ensure the ability to process multiple invoices through WAWF for less than the total obligated amount, the quantity and dollar value of all CLINS have been "flipped," i.e. 318,783.60 units @ $1. Vendor will invoice accordingly each month, i.e. 26,565.30 units @ $1.

The sum of all invoices submitted per Labor CLIN shall equal (and NOT exceed) the total CLIN amount

Wide Area Workflow (WAWF) instructions are noted below:

Invoicing In accordance with DFARS 252.232-7003, invoices must be submitted to the COR through Wide Area Workflow (WAWF). Inaccurate invoices shall be returned to the Vendor within seven (7) days for correction. Attachments created in a Microsoft Office product may be attached to the WAWF invoice (i.e. backup documentation such as monthly status reports, etc.). Maximum limit for size of each attachment file is 2 MB. Maximum file size per invoice is 5 MB. Additional information regarding WAWF may be found at https:\\wawf.eb.mil. Other invoice requirements are set forth in FAR 52.232-25.

The following information is provided for completion of invoices in WAWF:
PAY DODAAC: SL4701
WAWF Invoice Type 2 in 1
Inspection/Acceptance Point Inspection: Destination
Acceptance: Destination
Issue by DoDAAC: SP4703
Admin DoDAAC: SP4703
Inspect By DoDAAC: Leave Blank
Acceptor DoDAAC: SPM400
DCAA Auditor DoDAAC: Leave Blank

Email POC to include for WAWF notification: Douglas.Trostel@dla.mil

CONTINUED ON NEXT PAGE

SECTION B

SUPPLIES/SERVICES: R799-V00007640

ITEM DESCRIPTION:

See Attached Statement of Work.

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	R799-V00007640 Other Management Support Services	1,551,110.400	UN	$ 1.00	$ 1,551,110.40

PRICING TERMS: Firm Fixed Price

PREP FOR DELIVERY:

See Attached Statement of Work.

PERIOD OF PERFORMANCE: 04/09/2018 - 04/08/2019

SUPPLIES/SERVICES: R799-V00007640

ITEM DESCRIPTION:

See Attached Statement of Work.

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	R799-V00007640 Other Management Support Services	4,400.000	UN	$ 1.00	$ 4,400.00

PRICING TERMS: Firm Fixed Price

PREP FOR DELIVERY:

See Attached Statement of Work.

PERIOD OF PERFORMANCE: 04/09/2018 - 04/08/2019

GOVT USE

ITEM	PR	PRLI	External PR	External PRLI	External Material	Customer RDD/ Need Ship Date
0001	0072104455	0001	N/A	N/A	N/A	N/A
0002	0072104455	0001	N/A	N/A	N/A	N/A

* *

CONTINUED ON NEXT PAGE

SECTION A - SOLICITATION/CONTRACT FORM

52.204-16 COMMERCIAL AND GOVERNMENT ENTITY CODE REPORTING (JUL 2016) FAR

SECTION I - CONTRACT CLAUSES

52.203-19 PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017) FAR

52.204-14 SERVICE CONTRACT REPORTING REQUIREMENTS (OCT 2016) FAR

52.204-15 SERVICE CONTRACT REPORTING REQUIREMENTS FOR INDEFINITE-DELIVERY CONTRACTS (OCT 2016) FAR

52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (JUL 2016) FAR

52.204-19 INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014) FAR

52.204-20 PREDECESSOR OF OFFEROR (JUL 2016) FAR

As prescribed in 4.1804(d), insert the following provision:

(a) Definitions. As used in this provision -

“Commercial and Government Entity (CAGE) code” means -

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity; or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

“Predecessor” means an entity that is replaced by a successor and includes any predecessors of the predecessor.

“Successor” means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term “successor” does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

(b) The Offeror represents that it **[ ]** is or **[ ]** is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(c) If the Offeror has indicated “is” in paragraph (b) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code:

Predecessor legal name:

(Do not use a “doing business as” name)

(End of provision)

252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016) DFARS

(a) *Definitions.* As used in this clause -

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered defense information” means unclassified information that -

(1) Is -

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) Controlled technical information.

(ii) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(iii) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

(b) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to -

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) *Subcontracts*. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

(End of clause)

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016) DFARS

(a) *Definitions*. As used in this clause-

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

“Contractor information system” means an information system belonging to, or operated by or for, the Contractor.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria,

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified information that -

(i) Is --

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) *Controlled technical information*.

(B) *Critical information (operations security)*. Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

"Operationally critical support" means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall -

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum -

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government -

(A) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

Services, of this contract; and

(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause -

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and

(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement*.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall --

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) *Cyber incident report*. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information.* The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD.* Information that is obtained from the contractor

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD -

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD.* Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements.* The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall -

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and

(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

52.211-15 DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS (APR 2008) FAR

52.223-18 ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING (AUG 2011) FAR

52.232-33 PAYMENT BY ELECTRONIC FUNDS TRANSFER-SYSTEM FOR AWARD MANAGEMENT (JUL 2013) FAR

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013) FAR

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013) DFARS

As prescribed in 232.7004(b), use the following clause:

(a) *Definitions.* As used in this clause-

"Department of Defense Activity Address Code (DoDAAC)" is a six position code that uniquely identifies a unit, activity, or organization.
"Document type" means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).
"Local processing office (LPO)" is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) *Electronic invoicing.* The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) *WAWF access.* To access WAWF, the Contractor shall-

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.acquisition.gov; and
(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this web site.

(d) *WAWF training.* The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at https://wawf.eb.mil/

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(e) *WAWF methods of document submission.* Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) *WAWF payment instructions.* The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) *Document type.* The Contractor shall use the following document type(s).

_____

(Contracting Officer: Insert applicable document type(s).
Note: If a "Combo" document type is identified but not supportable by the Contractor's business systems, an "Invoice" (stand-alone) and "Receiving Report" (stand-alone) document type may be used instead.)

(2) *Inspection/acceptance location.* The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

_____

(Contracting Officer: Insert inspection and acceptance locations or "Not applicable.")

(3) *Document routing.* The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	
Issue By DoDAAC	
Admin DoDAAC	
Inspect By DoDAAC	
Ship To Code	
Ship From Code	
Mark For Code	
Service Approver (DoDAAC)	
Service Acceptor (DoDAAC)	
Accept at Other DoDAAC	
LPO DoDAAC	
DCAA Auditor DoDAAC	
Other DoDAAC(s)	

*(*Contracting Officer: Insert applicable DoDAAC information or "See schedule" if multiple ship to/acceptance locations apply, or "Not applicable.")*

(4) *Payment request and supporting documentation.* The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) *WAWF email notifications.* The Contractor shall enter the e-mail address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

_____

(Contracting Officer: Insert applicable email addresses or "Not applicable.")

(g) *WAWF point of contact.*

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

_____

(Contracting Officer: Insert applicable information or "Not applicable.")

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

(End of clause)

52.233-3 PROTEST AFTER AWARD (AUG 1996) FAR

252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013) DFARS

252.247-7023 TRANSPORATION OF SUPPLIES BY SEA (APR 2014) DFARS

52.253-1 COMPUTER GENERATED FORMS (JAN 1991) FAR